Carnegie Mellon
Software Engineering Institute

Home Search Contact Us Site Map What's New

Courses
Conferences
Building your skills
Licensing

About the SEI Management Engineering Acquisition Work with Us Products and Services Publications

PRODUCTS AND SERVICES

- Course Offerings
- Prices
- Locations and Travel Information
- Courses FAQ
- Registration
- Contact Information
- Credentials Program

Advanced Incident Handling for Technical Staff

Dates

2005 Dates

April 4-8, 2005 (SEI Pittsburgh, PA)
August 15-19, 2005 (Arlington, VA)
December 12-16, 2005 (SEI Pittsburgh, PA)

This course may also be offered by arrangement at customer sites. E-mail training-info@cert.org or call +1 412-268-9564 for details.

Prices (USD)

U.S.

Industry: $2625
Government: $2100
Academic: $2100

International

$5250

Course Registration

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
Phone: 412 / 268-7388
FAX: 412 / 268-7401
E-mail: courseregistration@sei.cmu.edu

2005
REGISTER

Course Description

This five-day course, designed for computer security incident response team (CSIRT) technical personnel with several months of incident handling experience, addresses commonly used and emerging attacks that are targeted against a variety of operating systems and architectures.

Building on the methods and tools discussed in the Fundamentals of Incident Handling course, this course provides steps that incident handlers can take in response to system compromises at the privileged level. Through interactive instruction, facilitated discussions, and group exercises, instructors help participants identify and analyze a set of events and then propose appropriate response strategies.

Participants work as a team throughout the week to handle a series of escalating incidents that are presented as part of an ongoing scenario. Work includes team analysis of information and presentation of findings and response strategies. Participants also review broader aspects of CSIRT work such as artifact analysis; vulnerability handling; and the development of advisories, alerts, and management briefings.

Before completing this course, participants are encouraged to attend the companion course, Fundamentals of Incident Handling. This course is part of the curriculum for the CERT-Certified Incident Handler program.

Audience · Prerequisites · Objectives · Logistics

AUDIENCE

- current computer security incident response team (CSIRT) members
- system and network administrators responsible for identifying and responding to security incidents

PREREQUISITES

Before registering for this course, it is recommended that participants have completed the Fundamentals of Incident Handling course (preferred). It is also recommended that participants have

- at least three months of incident handling experience
- experience with the administration of Windows and Unix systems
- an understanding of basic programming concepts and have experience programming in C, Perl, Java, or similar languages
- experience with various types of computer security attacks, response strategies, incident handling tools
- an understanding of Internet services and protocols

TOPICS

- review of critical information and typical probes and scans
- consequences of privileged compromises
- responding to and recovering from privileged compromises
- overview of typical intruder toolkits
- understanding distributed denial of service attacks
- handling major computer security events
- the role of artifact analysis in incident handling
- fundamental vulnerability causes
- vulnerability handling
- publishing CSIRT information
- security case study

OBJECTIVES

This course will help participants to

- detect and characterize various attack types
- gain practical experience in constructive analysis of artifacts left on a compromised system
- understand the complexity of and effectively respond to privileged and major event incidents within your CSIRT
- gain practical experience in the analysis of vulnerabilities and the coordination of vulnerability handling tasks
- formulate effective advisories, alerts, and management briefings

Course Materials

Participants will receive a course notebook and a CD containing the course materials.

LOGISTICS

Class Schedule

This five-day course meets at the following times:
Days 1-4, 9:00 a.m.-5:00 p.m.
Day 5, 9:00 a.m.-3:00 p.m.

Hotel and Travel Information

Information about traveling to SEI offices in Pittsburgh, Pennsylvania and Arlington, Virginia is available on our Travel and Lodging Web pages.

Questions about this course?

Please see our Frequently Asked Questions Web page for answers to some of the more common inquiries about SEI Education and Training. If you need more information, contact us via e-mail at training-info@cert.org or telephone at +1 412-268-9564.

Related Products and Services

Courses

Managing Computer Security Incident Response Teams (CSIRTs)
Creating a Computer Security Incident Response Team
Fundamentals of Incident Handling
Information Security for Technical Staff

Publications

CSIRT FAQ
CERT/CC Tech Tips
CERT/CC Current Activity
CERT/CC Overview Incident and Vulnerability Trends
CERT/CC Vulnerability Notes
The CERT® Guide to System and Network Security Practices

Events

Annual Computer Security Incident Handling Conference, sponsored by FIRST.ORG, Inc.

Other Related Information

CSIRT Development Information
CERT-Certified Incident Handler Certification
CERT Training and Education

Course Registration

2005

REGISTER

^
TOP

The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

URL: http://www.sei.cmu.edu/products/courses/cert/csih-advanced.html
Last Modified: 13 December 2004